A Seamless Handoff Mechanism for DHCP-Based IEEE 802.11 WLANs

Jen-Jee Chen, Yu-Chee Tseng, and Hung-Wei Lee

Abstract— **IEEE 802.11 wireless networks have gained great popularity. However, handoff is always a critical issue in this area. In this paper, we propose a novel seamless handoff mechanism for IEEE 802.11 wireless networks which support IEEE 802.11i security standard. Our approach consists of a *Dynamic Tunnel Establishing* procedure and a *seamless handoff* mechanism. Both intra- and inter-subnet handoff cases are considered in our seamless handoff approach. Our work focuses on handoffs in DHCP-based IP networks rather than Mobile IP-supported networks, but the proposed scheme can be easily tailored to Mobile IP-supported networks.**

Index Terms— **DHCP (Dynamic Host Configuration Protocol), dynamic tunnel, IEEE 802.11i, seamless handoff, wireless network.**

I. INTRODUCTION

IN recent years, IEEE 802.11 networks [1] have experienced rapid growth and popularity. Wireless networks offer access to the Internet for delivery of various services such as VoIP (voice over IP), multimedia, or data transmission. As a result, supporting user and device mobilities is a critical issue since continuous network connectivity is highly desirable for most services. However, supporting voice and multimedia with mobility implies that the total handoff latency must be small. The latency for VoIP should not exceed 50 ms to prevent excessive jitter [2], while streaming video/audio applications cannot tolerate a latency more than 150 ms [3].

Handoff refers to a mobile node (MN) moving from one AP's coverage to another. Generally, when a MN detects that its received signal strength (RSS) from its current AP has dropped below some certain threshold, it starts carrying out a wireless handoff. A wireless handoff is composed of 4 main phases: *Probe-and-Decision*, *Execution*, *DHCP (Dynamic Host Configuration Protocol)*, and *Upper Layer Adjustment*. In the Probe-and-Decision phase, the MN scans channels to find potential APs around it. After scanning, it will decide a target AP as its new AP according to some matrices such as RSS and loading. Then, the MN starts the Execution phase to attach to the target AP. In an IEEE 802.11i network [4], the Execution phase involves 3 steps: *reassociation*, *802.1x authentication*, and *four-way handshake*. During 802.1x authentication, the MN is authenticated to a backend authentication (AAA) server, such as RADIUS (Remote Authentication Dial-In User Service) server [5], via the new AP. If the authentication succeeds, both the MN and authentication server will derive the same PMK (Pairwise Master Key). The PMK is then transmitted to the new AP by the authentication server, which triggers the new AP to initiate the four-way handshake. In the four-way handshake, the MN and the new AP will derive several temporal keys, including a data encryption key and a data message integrity code (MIC) key, to protect data between the MN and the new AP. At this point, the link layer handoff is complete. That is, if the handoff occurs within the same IP subnet (an intra-subnet handoff), the handoff is finished after the Probe-and-Decision and Execution phases. The DHCP and Upper Layer Adjustment phases are needed when a MN moves from one IP subnet to another (an inter-subnet handoff). In this case, after the link layer handoff, the MN has to renew its IP address and reconfigure its network parameters with the DHCP server of the new IP subnet. Afterward, the MN executes the Upper Layer Adjustment phase to adjust its TCP/IP layer or applications in order to continue its original sessions. This completes the inter-subnet handoff.

Each phase mentioned above causes considerable delay. Experiments show latencies of 300-400 ms for the Probe-and-Decision phase, 800 ms for the 802.1x authentication, 40 ms for the four-way handshake, and 1-2 sec for the DHCP procedure [6]. Obviously, the total handoff delay is intolerable for real-time applications. In this paper, we investigate how to reduce handoff latency to provide seamless and continuous network connectivity.

A lot of research has tried to improve the latency of each handoff phase. For the Probe-and-Decision phase, mechanisms such as Neighbor Graph (NG)-based selective scanning [7], [8], SyncScan [9], and location-based fast handoff [10] have been presented. These schemes can effectively reduce the IEEE 802.11 probe latency from hundreds of ms to less than 20-30 ms. To accelerate the 802.1x authentication, the IEEE 802.11i standard [4] has included "Pre-authentication", which permits a MN to do pre-authentication with potential APs. Unfortunately, a MN can only pre-authenticate itself with APs on the same IP subnet. Reference [11] allows a MN to authenticate with multiple potential APs, rather than just its current AP. In order to select these potential APs (for pre-authentication), a mobility prediction is made, where an $O(n^2)$ analysis of RADIUS log information is required. Reference [12] presents a proactive key distribution scheme, which achieves a 99% reduction in the 802.1x authentication

Manuscript received April 16, 2007. The associate editor coordinating the review of this letter and approving it for publication was Prof. Carla-Fabiana Chiasserini.

J.-J. Chen is with the Department of Computer Science, National Chiao-Tung University, Taiwan (email: chencz@csie.nctu.edu.tw).

Y.-C. Tseng holds joint appointments at the Department of Computer Science, National Chiao-Tung University, Taiwan, and the Department of Information and Computer Engineering, Chung-Yuan Christian University, Taiwan (email: yctseng@cs.nctu.edu.tw). His research is co-sponsored by the Taiwan MoE ATU Program, by NSC grants 93-2752-E-007-001-PAE, 96-2623-7-009-002-ET, 95-2219-E-009-007, and 94-2219-E-007-009, by Zyxel Communications Corp., by MOEA under grant number 94-EC-17-A-04-S1-044, and by ITRI, Taiwan.

H.-W. Lee is with the ZyXEL Communications Corp., Taiwan (email: hewitt.lee@zyxel.com.tw).

Digital Object Identifier 10.1109/LCOMM.2007.070588.

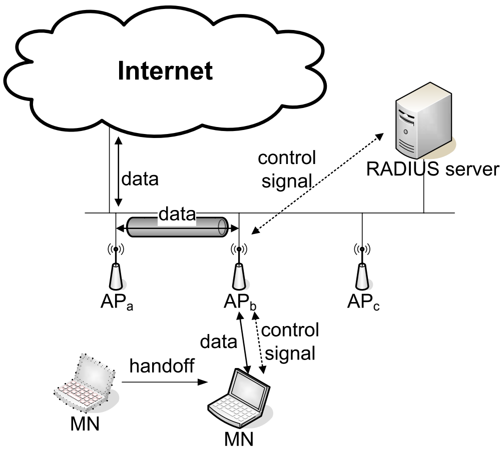

Fig. 1. System architecture.

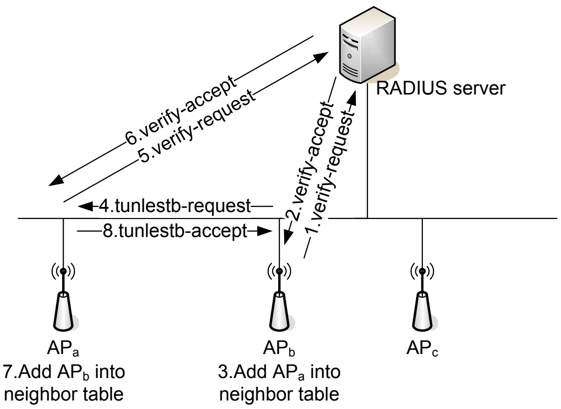

Fig. 2. Proposed Dynamic Tunnel Establishing procedure.

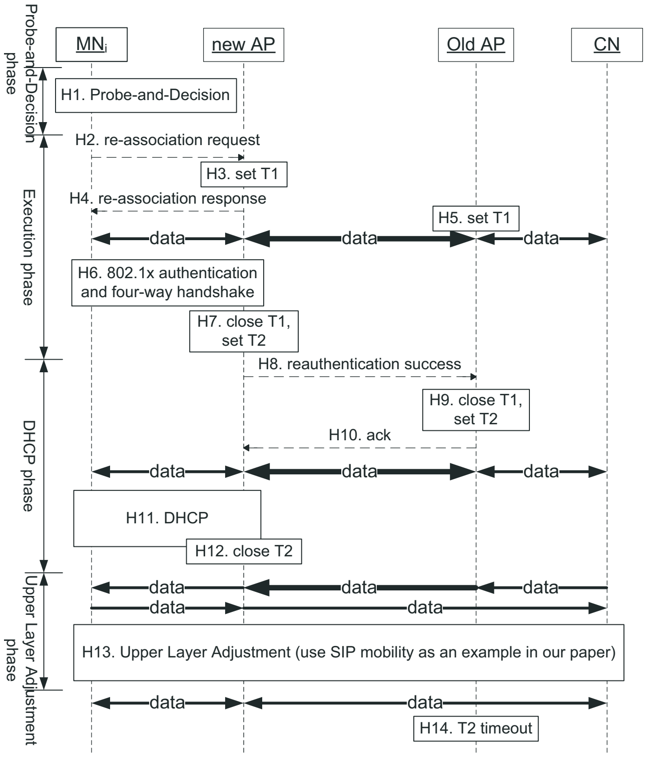

Fig. 3. Proposed seamless handoff mechanism.

time. However, it is unable to cooperate with current standard authentication processes, and needs to modify existing protocols.

II. Proposed Seamless Handoff Scheme

In the existing 802.1x authentication, users are not allowed to transmit/receive normal data via the new AP before the authentication succeeds. Considering that blocking normal data access can be done later on, we propose to allow a roaming MN to execute the 802.1x authentication and normal data access simultaneously for a short period of time. However, this may cause a security loophole. Hence, we enforce the MN to access the Internet via its previous AP before handoff completes. Since the previous AP has authenticated the MN, it can check if the MN is a legal user and provide the MN secure wireless access by using its prior data encryption key. Our approach consists of a *Dynamic Tunnel Establishing* procedure and a *seamless handoff* method. Dynamic Tunnel Establishing is for each AP to construct trusted tunnels with its neighbor APs. In the seamless handoff method, we propose to allow the roaming MN to access the Internet via its previous AP by the tunnel between the new AP and the previous one during the Execution, DHCP, and Upper Layer Adjustment phases of a handoff. Fig. 1 shows our proposed seamless handoff architecture, where a MN is moving from AP_a to AP_b. When the MN is authenticating with the RADIUS server via the new AP, AP_b, it also continues to access the Internet via its previous AP, AP_a. Therefore, we can achieve a seamless handoff for roaming MNs. Below, we will give an overview of our Dynamic Tunnel Establishing procedure and seamless handoff method.

Fig. 2 shows the Dynamic Tunnel Establishing procedure, which is triggered by the receipt of IEEE 802.11 *reassociation request* or IAPP *Move-Notify* message of AP_b. On receiving one of these two messages, AP_b finds that AP_a is its neighbor and then tries to establish a tunnel with AP_a. Before sending the request to AP_a, AP_b first verifies if AP_a is a trusted AP by querying its RADIUS server. If the verification succeeds, AP_b then sends AP_a a *tunlestb-request*. This tunlestb-request message asks AP_a to construct a layer-two tunnel if both APs are in the same subnet; otherwise, it asks AP_a to construct a layer-three tunnel. ARP (Address Resolution Protocol) can be used to determine whether both APs are in the same subnet or not. On the receipt of the tunlestab-request message, AP_a will also verify if AP_b is a trusted AP. If yes, AP_a will agree to establish the tunnel with AP_b.

Since the Dynamic Tunnel Establishing procedure is executed after the very first roaming MN handoffs from one AP to another, the first MN can not benefit from the seamless handoff method. However, later roaming MNs can all enjoy such tunneling services.

Next, let's see how the seamless handoff method works. Fig. 3 shows our seamless handoff mechanism, in which MN_i has a data connection with a corresponding node (CN) and it is moving from its old AP to a new AP. Here we assume that the SIP (Session Initiation Protocol) mobility [13] is used in the Upper Layer Adjustment phase. In our method, we do not propose an enhancement to the Probe-and-Decision phase because existing schemes already do well (such as the NG-based selective scanning [7], [8] and the SyncScan [9]). We can adopt one of them in the Probe-and-Decision phase (H1). After deciding the new AP, MN_i will send it a reassociation request message (H2). Upon the receipt of the reassociation request from MN_i, the new AP will be ready to relay data between the old AP and MN_i using the existing tunnel between it and the old AP. Here both the new AP and the old AP will set a timer *T1* as the threshold time to provide MN_i Internet access. Then, the new AP will reply MN_i a reassociation response and the 802.1x authentication starts (H6). Once T1 times out, if the 802.1x authentication does not complete, the relay will be prohibited by the new AP and the old AP. Notice that, before MN_i and the new AP derives a new data encryption key, MN_i will use the old key to encrypt data sent to the old AP. The new AP only tunnels the data to the old AP or forwards the encrypted data to MN_i. Once the 802.1x authentication and the four-way handshake complete, the new AP will close T1 (H7) and inform the old AP that the authentication has succeeded (H8). If this is an intra-subnet handoff, the seamless handoff procedure finishes; otherwise, this is an inter-subnet handoff and the new AP and the old AP will set a timer *T2* (in H7 and H9, respectively) to continue data relay for MN_i to maintain continuous network connectivity during executing remaining handoff procedures. The tunnel type between the old AP and the new AP can be used to determine whether the handoff is an intra- or inter-subnet handoff. Once T2 times out, the relay will be prohibited by the new AP and the old AP. Here we assume that some extension to DHCP for mobility support is implemented [14], [15], where the DHCP client in MN_i can detect the change of subnets. So, MN_i will actively execute the DHCP. After the link layer handoff, data is encrypted between MN_i and the new AP because a new data encryption key has been derived after the four-way handshake. On receiving the DHCP ACK message from the DHCP server of the new subnet (H11), the DHCP client will reconfigure MN_i's IP address and network parameters. Moreover, this will trigger the new AP to stop relaying uplink data to the old AP and start directly relaying uplink data from MN_i to the Internet because a new IP is used (H12). For the old AP, the downlink data forwarding from CN to the new AP is continued until T2 times out. Because CN will still transmit data to the old subnet before the SIP mobility competes, this can help MN_i to continue to receive downlink data. After the DHCP, MN_i will execute the SIP mobility procedure (H13). When the SIP mobility completes, CN will start to transmit data to the new subnet of MN_i. Then, the handoff procedure completes.

III. Conclusions

In this paper, we propose a Dynamic Tunnel Establishing procedure and a seamless handoff method to provide mobile users the seamless handoff and continuous network connectivity over DHCP-based IEEE 802.11 wireless networks which support IEEE 802.11i. During a handoff, by using our proposed approach, the Probe-and-Decision phase can be reduced to less than 20–30 ms by adopting one of existing schemes [7], [8], [9], [10], and the three remaining phases, Execution, DHCP, and Upper Layer Adjustment phases, can be hidden by the tunneling services. Therefore, for a roaming MN, the continuous disconnected period with the Internet can be guaranteed to be less than 50 ms. So, a seamless handoff is concluded. In addition, the proposed method provides the same security level as the original IEEE 802.11i standard because, during a handoff, the moving MN is allowed to access the Internet only when it is permitted by the old AP and the old AP is trusted. Moreover, if there's any improvement or change for the authentication and encryption methods, our seamless handoff mechanism still can work correctly because it doesn't involve any modification to the authentication and encryption methods.

References

[1] IEEE Std. 802.11, Nov. 1997.

[2] International Telecommunication Union, General Characteristics of International Telephone Connections and International Telephone Circuits, *ITU-TG.114*, 1988.

[3] L. Zan, J. Wang, and L. Bao, "Personal AP protocol for mobility management in IEEE 802.11 systems," in *Proc. 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MOBIQUITOUS)*, San Diego, CA, July 2005.

[4] IEEE Std. 802.11i, Nov. 2004.

[5] C. Rigney, S. Willens, A. Rubens, and W. Simpson, Remote Authentication Dial In User Service (RADIUS), *IETF RFC 2865*, June 2000.

[6] B. Aboba, Fast Handoff Issues, IEEE-03-155r0-I, *IEEE 802.11 Working Goup*, March 2003.

[7] M. Shin, A. Mishra, and W. A. Arbaugh, "Improving the latency of 802.11 handoffs using neighbor graphs," in *Proc. 2nd Int'l Conference on Mobile Systems, Applications, and Services (MobiSys2004)*, pp. 70–83, June 2004.

[8] P.-J. Huang, Y.-C. Tseng, and K.-C. Tsai, "A fast handoff mechanism for IEEE 802.11 and IAPP networks," in *Proc. VTC2006-Spring*, vol. 2, pp. 966–970, 2006.

[9] I. Ramani and S. Savage, "SyncScan: practical fast handoff for 802.11 infrastructure networks," in *Proc. INFOCOM2005*, vol. 1, pp. 675–684, March 2005.

[10] C.-C. Tseng, K.-H. Chi, M.-D. Hsieh, and H.-H. Chang, "Location-based fast handoff for 802.11 networks," *IEEE Commun. Lett.*, vol. 9, no. 4, pp. 304–306, Apr. 2005.

[11] S. Pack and Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems," *IEEE Proc. Commun.*, vol. 151, no. 5, pp. 489–495, Oct. 2004.

[12] A. Mishra, M. H. Shin, N. L. Petroni, T. C. Clancy, and W. A. Arbaugh, "Proactive key distribution using neighbor graphs," *IEEE Trans. Wireless Commun.*, pp. 26–36, Feb. 2004.

[13] F. Vakil, A. Dutta, and J. C. Chen, "Supporting mobility for multimedia with SIP," *draft-itsumo-sipping-mobility-multimedia-01.txt*, July 2001.

[14] A. Floris, L. Tosetti, and L. Veltri, "Solutions for mobility support in DHCP-based environments," in *Proc. IEEE ICC'03*, pp. 1043–1047.

[15] A. McAuley and K. Manousakis, "Self-configuring networks," in *Proc. 1st Century Military Communications Conference (MILCOM 2000)*, vol. 1, pp. 315–319, 2000.